SUGGESTED PRESENTATION BY THE DIRECTOR AT NSA

DURING NSA'S TENTH ANNUAL SECURITY WEEK

Good Afternoon.

I welcome the opportunity to participate in your Tenth Annual Security Week Program. In the climate of permissiveness and dissension that exists now not only in this country but around the world, security must be a serious concern to us all.

The intelligence organs of the Soviet Union and the Chinese Communists and their satellites, or the "opposition" as we have come to refer to them, have become increasingly pervasive and sophisticated. There is no country in the free world today where at least one of them is not actively pursuing a program of espionage. This is particularly true of the Soviet Union's KGB which has increased steadily its official representation in the non-communist countries of the world. It is widely known that the United States is the top priority objective of the KGB and that key elements of the American

intelligence services, such as the Federal Bureau of Investigation, the Central Intelligence Agency, and the National Security Agency head its list of targets.

The number of Soviet officials assigned to the United States -- in the Embassy in Washington, in the Soviet Mission to the United Nations, and to various ancillary establishments, such as AMTORG and Tass -- has more than doubled over the past ten years. In September of 1961, more than 300 such officials were present in this country. There are now more than 700. This increase in representation is of real concern, particularly when we know that a variety of reliable sources have, over the years, estimated that more than 70 percent of the Soviets in this country have some intelligence mission.

We in the United States are not alone in our awareness to the omnipresent Soviet threat. The most dramatic aftereffect of the defection of Oleg Adolfovich Lyanin, a 34 year old KGB officer to the British Government in early September 1971, was the announcement by the British Foreign Office that it had demanded the removal of 90 Soviet representatives from Great

Britain and was denying re-entry to some 15 others who were temporarily away from their posts in Britain. In announcing the move, the Foreign Office released the text of letters it had written to the Soviets in December 1970 and August 1971, in which it had protested "large scale espionage" being conducted by the Soviets in Great Britain.

While we're at it, let's not overlook the collection efforts of our friends. Particularly in our liaison activities must we not relax and fall into sloppy habits. What we're doing, how we're doing it, and, obviously, what we know are of deep and abiding interest to all of them, be they the French, the Argentines, the Israelis, the Belgians. Courteous reticence should be the style of our intercourse.

In the face of these threats, I think it is important that all of us who are so vitally concerned with the security of this country and particularly protection of classified intelligence information and sources, periodically

re-examine and re-evaluate our security practices and attentiveness to ensure that everything that can be done is being done to maintain the national security, including the integrity of our intelligence mission.

There are many elements to security. If I were asked which is the most important, I would have to say that it is the security of our personnel. It may be trite but it is most certainly axiomatic that the security chain is only as strong as its weakest link. Despite all of the advancements we have made in recent years in physical and technical security and despite all of the precautions we take in other related fields, one "bad apple in the barrel" can cause near irreparable damage. You have all seen, over the years, tangible evidence that the United States intelligence community can be penetrated. The "can happen heres" include such well-known espionage cases as Jack Dunlap, Robert Thompson, Robert Lee Johnson, James Allen Mintkenbaugh, Colonel Whelan, and most recently, the allegation of espionage against Air

Force Sgt. Walter Perkins. Indeed I think that the job of being a case officer for the KGB in the free world must be a relatively easy one. I have often told my operational people that if it were as easy for us to conduct our activities against the opposition we would be in an enviable position.

In the Central Intelligence Agency, we operate our personnel security program on the assumption that the Agency can be penetrated and we spend considerable time, in conjunction with the Federal Bureau of Investigation, in conducting investigations of alleged penetrations. Fortunately, the cases we have investigated thus far have been resolved in favor of the employee. The fact that we have not yet unearthed a paid agent of a foreign intelligence service at work in the Agency is not at all reassuring but acts rather as a spur to keep us attuned and alert to the ever present possibility that we may, in fact, have a spy in our midst.

All of us must keep constantly in mind the fact that because of current dissemination practices and the extensive coordination of both raw and finished intelligence, a penetration of any one agency usually involves the compromise of classified material of others. The Sgt. Johnson case is an excellent example of this. Although he was assigned to the Armed Forces Courier Service when he turned over classified information to the KGB, the material included sensitive reports of several agencies.

All of us in the intelligence business operate from the same basic framework in clearing our employees, with a possible exception that some of us use the polygraph and some do not. Our field investigations are generally thorough and comprehensive, and our security clearances are issued in accordance with the provisions of Executive Order 10450. Personnel security however does not stop when an employee is safely on board. We cannot sit back complacently and assume that because our employees have been through our security screening programs they will be

good security risks during the rest of their careers. People change as they mature; personal and job-related problems occur just as they do with each of you and with me. Most people handle their problems intelligently and discreetly enough to keep these problems from assuming any security significance but others do not. It is those few who, because of human frailty and weakness, are most susceptible to the ever present aggressive attempts at exploitation or penetration by the opposition.

Of all the Americans who have been discovered to have been successfully recruited by the KGB as espionage agents, with the possible exception of the Rosenbergs, none was ideologically motivated. Rather, the approach has been to a weakness of character, discretion or integrity. A close examination shows the motivations have been money, sex, revenge, alcohol or other evidences of basic psychological weakness. Human weaknesses have always existed and will continue to exist. They are the

soft spots in security and will be tested and threatened -- both by the opposition and by the pressures and demands of our own society.

Human weaknesses such as these assume far greater security significance among our personnel assigned abroad. The National Security Agency and the Central Intelligence Agency together staff installations in almost every country of the world and our people are more exposed to the painstaking surveillance of hostile intelligence services. We have all heard of recruitment attempts, kidnappings and even assassination. It behooves us, therefore, to make sure that the personnel we assign overseas are carefully screened from the outset and that they are continually indoctrinated in sound principles of personal security so that they can not only resist attempts at exploitation in this country, but more specifically when they are assigned to a hostile environment somewhere on the other side of the globe.

Before I leave the subject of personnel security, I would like to stress a few factors which I am convinced must provide the basis for our continuing review of our personnel security programs. First, is the importance of the role of the supervisor. A good supervisor who regards the people who work for him as human beings, subject to pressures, tension and stress instead of just mechanical tools, is one of our strongest security assets. I am not advocating a "buddy-buddy" or forced social relationship with those with whom you work or who work for you. I am advocating that every supervisor know his people well enough that changes in their behavior patterns, which may have potential security significance, can be recognized. Many of our supervisors have been able to recognize and assist their employees with problems, which, if disregarded, might have worsened to the point where they could have become a definite security risk.

Secondly, and this is in accord with the theme of your program this year, is that any good personnel security program must be a flexible one.

We must recognize that the people we are hiring today, while just as highly motivated and just as patriotic as those we hired twenty years ago, have been raised and educated in a different world. We cannot force them into rigid patterns by regulation alone. We must, without any compromise of basic security standards, modify our regulations realistically and intelligently to reflect changing attitudes in changing times. I am convinced that the young people we are hiring today in the intelligence profession are just as sound as those we hired twenty years ago. They are also badly needed to inject the new ideas and imagination that will keep the intelligence profession a viable and effective one.

Finally, a good personnel security program must be administered in a positive sense, with liberal application of sympathy and human understanding. The most effective security service is one that is recognized as a "friendly security service" whose first concern is the interest of the employees and the

preservation of their human dignity. If the security service is administered in this fashion, employees will bring their problems to security personnel with confidence and trust. In our society a security service which employs a "Gestapo" approach has lost the race before it starts.

There is another area of security which must be considered of vital interest to all of us in the intelligence profession. I refer to the increasingly frequent and extensive compromise of intelligence information through unauthorized disclosures of classified information in the public media, primarily the press. Since 1957, more than 100 articles have appeared in the public press containing classified intelligence information warranting surveys or investigations by the Security Committee of the United States Intelligence Board. Between January 18 and May 27, 1971, twenty-two specific unauthorized disclosures appeared in the public press. This represents the highest rate in the history of the intelligence community for any equivalent period.

What is the effect of these disclosures and what is their significance to us as professional intelligence officers? Obviously, this free flow of classified information gives the Soviet Union and other foreign powers gratuitous insight into the capabilities and limitations of our intelligence system. More importantly, I believe, it serves to undermine at all levels of government the importance of maintaining our security integrity.

It is extremely difficult and usually impossible to conduct a successful investigation of unauthorized disclosures. The chief reason for this is the wide dissemination given intelligence products within the intelligence community and the United States Government. Any thorough security investigation would, in many cases, involve interviewing literally thousands of consumers. Almost without exception investigations of such disclosures by investigative elements of the departments and agencies represented on the United States Intelligence Board have been unsuccessful.

In a practical sense we have had to turn to other means of tightening our security and maintaining the integrity of our intelligence information. Over the years, I have given considerable thought to the motivation behind such disclosures. Some of them are discernible during prolonged and intense debate over a particular budget item or other major policy issue and I am sure that many disclosures have been made in a misguided effort to evoke favorable action by the Congress or elements of the Executive Branch of our Government. I am sure you will agree with me that the cumulative effect is insidious and has tended to undermine public confidence in the manner in which the United States Government conducts its affairs. I am sure that all of you have your own views on this subject but I will say that it is a very poor state of affairs indeed when one individual assumes the responsibility for deciding that he alone knows best what is in the national interest.

The President has expressed grave concern about the proliferation of unauthorized disclosures in the press. He has charged all United States departments and agencies with the responsibility for taking drastic action. Specifically, he has directed that immediate review be made of all personnel having special or compartmented clearances with a view toward reducing the number of these clearances to an absolute minimum consistent with "need-to-know". He has also created a special committee under the chairmanship of Mr. William Rehnquist of the Department of Justice to review and recommend changes in Executive Order 10501 which contains procedures governing the classification and declassification of documents in the United States Government.

As the Chairman of the United States Intelligence Board and as Director of Central Intelligence, I have taken a number of actions to close this gap in the security of the intelligence community. I have made repeated

requests to members of the Board that requirements for the dissemination of intelligence information continually be reviewed and limited; that special clearances be held to the minimum; and that personnel be reindoctrinated periodically on the need for security. I hope that these actions have had some effect but in the final analysis each individual employee who has access to classified intelligence information must take upon himself the responsibility for ensuring that he maintains the integrity of the privileged information to which he has access. I urge each of you to assume this responsibility fully and hope that you will continue to work individually and collectively to stop this ill-reasoned and illegitimate distortion of security standards.